

# A Successive Resultant Projection for Cylindrical Algebraic Decomposition

**Yong Yao**

*Chengdu Institute of Computer Applications, Chinese Academy of Sciences, Chengdu,  
Sichuan 610041, PR China E-mail: yaoyong@casit.ac.cn*

**Jia Xu**

*College of Computer Science and Technology, Southwest University for Nationalities, Chengdu,  
Sichuan 610041, PR China E-mail: jjiaxu@gmail.com*

**Lu Yang**

*Chengdu Institute of Computer Applications, Chinese Academy of Sciences, Chengdu,  
Sichuan 610041, PR China E-mail: luyang@casit.ac.cn*

**Abstract** This note shows the equivalence of two projection operators which both can be used in cylindrical algebraic decomposition (CAD). One is known as Brown's Projection (C. W. Brown (2001)); the other was proposed by Lu Yang in his earlier work (L. Yang and S. H. Xia (2000)) that is sketched as follows: given a polynomial  $f$  in  $x_1, x_2, \dots$ , by  $f_1$  denote the resultant of  $f$  and its partial derivative with respect to  $x_1$  (removing the multiple factors), by  $f_2$  denote the resultant of  $f_1$  and its partial derivative with respect to  $x_2$ , (removing the multiple factors),  $\dots$ , repeat this procedure successively until the last resultant becomes a univariate polynomial. Making use of an identity, the equivalence of these two projection operators is evident.

**Keywords** cylindrical algebraic decomposition (CAD), projection operator, resultant.

**MR(2000) Subject Classification** 12Y05, 13P15, 14P10, 68W30

## 1 Introduction

Cylindrical algebraic decomposition (CAD) is a key constructive tool in real algebraic geometry. Given such a decomposition in  $\mathbb{R}^n$  it is easy to obtain a solution of a given semi-algebraic system. The CAD-algorithm was established by Collins [1] in 1975 as the basis of his quantifier elimination method in real closed fields and has been improved over the years (see [2],[3],[4],[5],[6],[7]).

CAD construction proceeds in two phases, projection and lifting. The projection phase computes a set of polynomials called *projection factor set* which consists of the irreducible factors of given polynomials. The focus of this note is projection phase, while lifting phase is not described. The readers are referred to (Collins, 1988 [1]; Collins and Hong, 1991 [4]) for a detailed description of the lifting phase.

## 2 An identity involving resultants, discriminants and leading coefficients

We require a number of well-known definitions which can be found in some books ([8], [9]).

---

The work was partially supported by the National Key Basic Research Project of China (GrantNo. 2011CB302402) and the Fundamental Research Funds for the Central Universities, Southwest University for Nationalities (GrantNo.12NZYTH04).

Let  $f$  and  $g$  be two non-zero polynomials of degree  $n$  and  $m$  in  $\mathbb{R}[x]$ .

$$\begin{aligned} f &= a_n x^n + \cdots + a_0, \\ g &= b_m x^m + \cdots + b_0. \end{aligned}$$

We define the Sylvester matrix associated to  $f$  and  $g$  and the resultant of  $f$  and  $g$  as follows.

**Definition 1** The Sylvester matrix of  $f$  and  $g$ , denoted by  $\mathbf{S}(f, g)$ , is the matrix

$$\mathbf{S}(f, g) = \begin{pmatrix} a_n & \cdots & \cdots & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & \ddots & & & & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & & & \ddots & 0 \\ 0 & \cdots & 0 & a_n & \cdots & \cdots & \cdots & \cdots & a_0 \\ b_m & \cdots & \cdots & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & & & & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & b_m & \cdots & \cdots & \cdots & b_0 \end{pmatrix}.$$

It has  $m + n$  columns and  $m + n$  rows. The **resultant** of  $f$  and  $g$ , denoted by  $\text{Res}(f, g, x)$ , is the determinant of  $\mathbf{S}(f, g)$ .

The other formula on  $\text{Res}(f, g, x)$  is as follows. If  $a_n \neq 0$  and  $b_m \neq 0$  then

$$\text{Res}(f, g, x) = a_n^n b_m^m \prod_{i=1}^n \prod_{j=1}^m (x_i - y_j) = (-1)^{mn} \text{Res}(g, f, x), \quad (1)$$

where  $x_1, \dots, x_n$  are roots of  $f$  and  $y_1, \dots, y_m$  are roots of  $g$  in  $\mathbb{C}$ .

**Definition 2** Let  $f \in \mathbb{R}[x]$  be a polynomial of degree  $n$ ,

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0,$$

and let  $x_1, \dots, x_n$  be the roots of  $f$  in  $\mathbb{C}$  (repeated according to their multiplicities). The **discriminant** of  $f$ ,  $\text{Dis}(f)$ , is defined by

$$\text{Dis}(f, x) = (-1)^{\frac{n(n-1)}{2}} a_n^{2n-2} \prod_{n \geq i > j \geq 1} (x_i - x_j)^2. \quad (2)$$

The following proposition holds clearly from (1) and Definition 2.

By  $f'$  denote the derivative of  $f$ , here

$$f' = n a_n x^{n-1} + \cdots + a_1.$$

Then we have the following formula

$$\text{Res}(f, f', x) = a_n \text{Dis}(f, x) = \text{Lc}(f, x) \cdot \text{Dis}(f, x), \quad (3)$$

where  $\text{Lc}(f, x)$  is the leading coefficient.

Using the equations (1) and (2) the following equation may be easily proved,

$$\text{Res}(fg, (fg)', x) = \text{Res}(f, f', x) \cdot \text{Res}(g, g', x) \cdot \text{Res}(f, g, x) \cdot \text{Res}(g, f, x). \quad (4)$$

The equation (4) is also equivalent to the classical formula ( I. M. Gelfand, M. M. Kapranov,

A. V. Zelevinsky (1994), P405,(1.32) [8] )

$$\text{Res}(f, g, x)^2 = (-1)^{mn} \frac{\text{Dis}(fg, x)}{\text{Dis}(f, x)\text{Dis}(g, x)}.$$

**Example 1.** Let  $f = ax^2 + bx + c$  and  $g = a_1x^2 + c_1$  in  $\mathbb{R}[x]$ . Then the equation (4) is the following.

$$\begin{aligned} & \left| \begin{pmatrix} aa_1 & ba_1 & (ac_1 + ca_1) & bc_1 & cc_1 & 0 & 0 \\ 0 & aa_1 & ba_1 & ac_1 + ca_1 & bc_1 & cc_1 & 0 \\ 0 & 0 & aa_1 & ba_1 & ac_1 + ca_1 & bc_1 & cc_1 \\ 4aa_1 & 3a_1b & (2ac_1 + 2a_1c) & bc_1 & 0 & 0 & 0 \\ 0 & 4aa_1 & 3a_1b & (2ac_1 + 2a_1c) & bc_1 & 0 & 0 \\ 0 & 0 & 4aa_1 & 3a_1b & (2ac_1 + 2a_1c) & bc_1 & 0 \\ 0 & 0 & 0 & 4aa_1 & 3a_1b & (2ac_1 + 2a_1c) & bc_1 \end{pmatrix} \right| \\ &= \left| \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix} \right| \cdot \left| \begin{pmatrix} a_1 & 0 & c_1 \\ 2a_1 & 0 & 0 \\ 0 & 2a_1 & 0 \end{pmatrix} \right| \cdot \left| \begin{pmatrix} a & b & c & 0 \\ 0 & a & b & c \\ a_1 & 0 & c_1 & 0 \\ 0 & a_1 & 0 & c_1 \end{pmatrix} \right| \cdot \left| \begin{pmatrix} a_1 & 0 & c_1 & 0 \\ 0 & a_1 & 0 & c_1 \\ a & b & c & 0 \\ 0 & a & b & c \end{pmatrix} \right| \end{aligned}$$

**Remark 1.** Note that the equation of Example 1 is an identity relative to  $a, b, c, a_1, c_1$ . In other words, the equation (4) still holds when we replace the ring  $\mathbb{R}[x]$  with the ring  $\mathbb{R}[x_1, \dots, x_n]$  and the variable  $x$  with  $x_i$ . The book Algebra (M. Artin (1991), pages 456-457. [12]) has a very brilliant discussion how to give a strict proof of this kind of identities.

We present a key Lemma now .

**Lemma 1** Let  $s \geq 2, k \geq 2$  and let  $f, f_1, \dots, f_s$  be squarefree polynomials of positive degree in  $\mathbb{R}[x_1, \dots, x_k]$ . Then the following two identities hold,

$$\text{Res}(f, \frac{\partial(f)}{\partial x_1}, x_1) = \text{Lc}(f, x_1) \cdot \text{Dis}(f, x_1). \quad (5)$$

$$\text{Res}(\prod_{i=1}^s f_i, \frac{\partial(\prod_{i=1}^s f_i)}{\partial x_1}, x_1) = \prod_{i=1}^s \text{Lc}(f_i, x_1) \cdot \prod_{i=1}^s \text{Dis}(f_i, x_1) \cdot \prod_{i \neq j \leq s} \text{Res}(f_i, f_j, x_1). \quad (6)$$

Where Lc, Dis and Res denote the leading coefficients, discriminants and resultants respectively.

**Proof** It is clear that the identity (5) comes from (3).

The following is the proof of (6) by induction on the number of polynomials  $s$ .

Base case:  $s = 2$ .

From (4), (5) and Remark 1, we have

$$\begin{aligned} & \text{Res}(f_1 f_2, \frac{\partial(f_1 f_2)}{\partial x_1}, x_1) \\ &= \text{Res}(f_1, \frac{\partial(f_1)}{\partial x_1}, x_1) \cdot \text{Res}(f_2, \frac{\partial(f_1)}{\partial x_1}, x_1) \cdot \text{Res}(f_1, f_2, x_1) \cdot \text{Res}(f_2, f_1, x_1) \\ &= \text{Lc}(f_1, x_1) \cdot \text{Lc}(f_2, x_1) \cdot \text{Dis}(f_1, x_1) \cdot \text{Dis}(f_2, x_1) \cdot \text{Res}(f_1, f_2, x_1) \cdot \text{Res}(f_2, f_1, x_1). \end{aligned}$$

Induction step: suppose  $s = t > 2$ , the following holds,

$$\text{Res}\left(\prod_{i=1}^t f_i, \frac{\partial(\prod_{i=1}^t f_i)}{\partial x_1}, x_1\right) = \prod_{i=1}^t \text{Lc}(f_i, x_1) \cdot \prod_{i=1}^t \text{Dis}(f_i, x_1) \cdot \prod_{i \neq j \leq t} \text{Res}(f_i, f_j, x_1). \quad (7)$$

From (5) we have the identity

$$\text{Lc}\left(\prod_{i=1}^t f_i, x_1\right) \cdot \text{Dis}\left(\prod_{i=1}^t f_i, x_1\right) = \text{Res}\left(\prod_{i=1}^t f_i, \frac{\partial(\prod_{i=1}^t f_i)}{\partial x_1}, x_1\right). \quad (8)$$

From the base case  $s=2$  we have

$$\begin{aligned} & \text{Res}\left(\prod_{i=1}^{t+1} f_i, \frac{\partial(\prod_{i=1}^{t+1} f_i)}{\partial x_1}, x_1\right) \\ &= \text{Lc}\left(\prod_{i=1}^t f_i, x_1\right) \cdot \text{Lc}(f_{t+1}, x_1) \cdot \text{Dis}\left(\prod_{i=1}^t f_i, x_1\right) \cdot \text{Dis}(f_{t+1}, x_1) \cdot \text{Res}\left(\prod_{i=1}^t f_i, f_{t+1}, x_1\right) \\ & \quad \cdot \text{Res}(f_{t+1}, \prod_{i=1}^t f_i, x_1) \\ &= \text{Res}\left(\prod_{i=1}^t f_i, \frac{\partial(\prod_{i=1}^t f_i)}{\partial x_1}, x_1\right) \cdot \text{Lc}(f_{t+1}, x_1) \cdot \prod_{i=1}^{t+1} \text{Dis}(f_i, x_1) \cdot \text{Res}\left(\prod_{i=1}^t f_i, f_{t+1}, x_1\right) \\ & \quad \cdot \text{Res}(f_{t+1}, \prod_{i=1}^t f_i, x_1). \end{aligned}$$

We need yet the multiplicativity of resultant ([8]).

$$\text{Res}\left(\prod_{i=1}^t f_i, f_{t+1}, x_1\right) = \prod_{i=1}^t \text{Res}(f_i, f_{t+1}, x_1). \quad (9)$$

$$\text{Res}(f_{t+1}, \prod_{i=1}^t f_i, x_1) = \prod_{i=1}^t \text{Res}(f_{t+1}, f_i, x_1). \quad (10)$$

Using the inductive hypothesis (7) and the equations (9) , (10), we obtain at once that

$$\text{Res}\left(\prod_{i=1}^{t+1} f_i, \frac{\partial(\prod_{i=1}^{t+1} f_i)}{\partial x_1}, x_1\right) = \prod_{i=1}^{t+1} \text{Lc}(f_i, x_1) \cdot \prod_{i=1}^{t+1} \text{Dis}(f_i, x_1) \cdot \prod_{i \neq j \leq t+1} \text{Res}(f_i, f_j, x_1).$$

The proof is completed.

### 3 The equivalence of two projection for CAD

The first projection **Proj** comes from C.W. Brown (2001) [6].

**Definition 3** (C. W. Brown (2001)) Let  $A$  be a squarefree basis in  $\mathbb{Z}[x_1, \dots, x_k]$ , where  $k \geq 2$ . Define the projection  $\text{Proj}(A, x_j)$  of  $A$  to be the union of the set of all leading coefficients of elements of  $A$  in variable  $x_j$ , the set of all discriminants of elements  $f$  of  $A$  in variable  $x_j$ , and the set of all resultants of pairs  $f, g$  of distinct elements of  $A$  in variable  $x_j$ .

$P \leftarrow \mathbf{Projection\ 1}(A)$  (Proj, C.W. Brown (2001))

Input:  $A \subseteq \mathbb{R}[x_1, \dots, x_k]$

Output:  $P$ , the projection factor set of a sign-invariant CAD for  $A$ .

- (1)  $P_0 := \text{IrreducibleFactorsOf}(A)$ ,  $P := P_0$ .
- (2) for  $j$  from 1 to  $k - 1$  do
  - $P_j := \text{IrreducibleFactorsOf}(\text{Proj}(P_{j-1}, x_j))$
  - $P := P \cup P_j$ .
- (3) Return  $P$ .

The other projection **ResP** comes from L. Yang *et al.* (2000, 2001) [11],[12].

**Definition 4** (L. Yang *et al.* (2000)) Let  $A$  be a squarefree basis in  $\mathbb{Z}[x_1, \dots, x_k]$ , where  $k \geq 2$ . Define the projection  $\text{ResP}(A, x_j)$  of  $A$  to be the squarefree polynomial, which is the product of irreducible factors of the resultant

$$\text{Res}\left(\prod_{\alpha \in A} \alpha, \frac{\partial(\prod_{\alpha \in A} \alpha)}{\partial x_j}, x_j\right).$$

$P \leftarrow \mathbf{Projection\ 2}(A) \quad (\text{ResP})$

Input:  $A \subseteq \mathbb{R}[x_1, \dots, x_k]$

Output:  $P$ , the projection factor set of a sign-invariant CAD for  $A$ .

- (1)  $P_0 := \text{IrreducibleFactorsOf}(A)$ ,  $P := P_0$ .
- (2) for  $j$  from 1 to  $k - 1$  do
  - $P_j := \text{IrreducibleFactorsOf}(\text{ResP}(P_{j-1}, x_j))$
  - $P := P \cup P_j$ .
- (3) Return  $P$ .

According to Lemma 1, it is clear that the projection  $\text{Proj}$  and  $\text{ResP}$  generate the same projection factor set. So they are equivalent for CAD.

#### 4 ResP for one polynomial

The projection  $\text{ResP}$  is firstly applied to solving the global optimization problems for algebraic functions by L. Yang *et al.* (2000, 2001)[11],[12]. Recently, J. J. Han, L. Y. Dai, B. C. Xia (2014) [7] improve the method by adding GCD computation. In the same paper, they have proved that improved HP ( $\text{ResP}$ ) still guarantees obtaining at least one sample point from every connected component of the highest dimension.

Using the projection  $\text{ResP}$  to only one polynomial  $f \in \mathbb{R}[x_1, \dots, x_n]$ , we can usually obtain a triangular system, the real zeros of which contain all of the real critical points of  $f$ . Namely the real zeros of the system

$$\begin{cases} f = 0, \\ \frac{\partial(f)}{\partial x_1} = 0, \\ \dots \\ \frac{\partial(f)}{\partial x_n} = 0. \end{cases}$$

must satisfy the following triangular system

$$\begin{cases} f = 0, \\ \text{ResP}(f, x_1) = 0, \\ \dots \\ \text{ResP}(\dots \text{ResP}(\text{ResP}(f, x_1), x_2) \dots, x_{n-1}) = 0. \end{cases}$$

For the polynomial  $f - T$  (where  $f \in \mathbb{R}[x_1, \dots, x_n]$ ), the equation

$$\text{ResP}(\cdots \text{ResP}(\text{ResP}(f - T, x_1), x_2) \cdots, x_n) = 0 \quad (11)$$

is of only a variable  $T$ . If the optimal value of function  $f$  exists in  $\mathbb{R}^n$ , say  $f_{\min}$ , then  $f_{\min}$  has to satisfy equation (11).

## References

- [1] G. E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In *Second GI Conference Automata Theory and Formal Languages, Kaiserslauten*, Volume 33 of Lecture Notes Comp. Sci., pages 134-183. Springer, 1975.
- [2] S. McCallum. An improved projection operation for cylindrical algebraic decomposition of three-dimensional space. *J. Symb. Comput.* 5(1): 141-161, 1988.
- [3] H. Hong. A Improvement of the projection operator in cylindrical algebraic decomposition. In *proceedings ISSAC'90*, 261-264, 1990.
- [4] G. E. Collins, H. Hong. Partial cylindrical algebraic decomposition for quantifier elimination. *J. Symb. Comput.*, 12(3): 299-328, 1991.
- [5] S. McCallum. An improved projection operation for cylindrical algebraic decomposition. In *Quantifier Elimination and Cylindrical Algebraic Decomposition*, 242-268, Springer, 1998.
- [6] C. W. Brown. Improved projection for cylindrical algebraic decomposition. *J. Symb. Comput.* 32(5): 447-465, 2001.
- [7] J. J. Han, L. Y. Dai, B. C. Xia. Constructing fewer open cells by GCD computation in CAD projection. In *Proc. ISSAC'14*, 240-247, 2014.
- [8] I. M. Gelfand, M. M. Kapranov, A. V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants*. Boston: Birkhäuser, 1994.
- [9] L. Yang, B. Xia, *Automated Proving and Discovering on Inequalities* (in Chinese). Beijing: Science Press, 2008.
- [10] M. Artin. *Algebra*. Englewood Cliffs: Prentice Hall, 1991.
- [11] L. Yang, S. H. Xia. An inequality-proving program applied to global optimization. In *Proceedings of ATCM 2000*, W-C. Yang *et al* (eds.), ATCM, Inc., Blacksburg, 40-51, 2000.  
(Also see <http://epatcm.any2any.us/EP/EP2000/ATCMP208/fullpaper.pdf>)
- [12] L. Yang. A symbolic algorithm for optimization and finiteness principle. In *Mathematics and Mathematics Mechanization*, D. D. Lin *et al* (eds). Jinan: Shandong Educational Publishing House, 2001.  
(Also see <http://book.lh.chaoxing.com/ebook/detail.jhtml?id=10924129&page=210>)